IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK

MARY COGAN, *individually and on behalf of all others similarly situated*, Plaintiff, v. SKIDMORE COLLEGE, Defendant.	Case No. 1:23-cv-1409 (MAD/DJS) **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Mary Cogan ("Plaintiff"), individually and on behalf of all others similarly situated (the "Class"), brings this Class Action Complaint against Defendant Skidmore College ("Defendant"). The allegations in this Complaint are based on the personal knowledge of the Plaintiff and upon information and belief and further investigation of counsel.

NATURE OF THE ACTION

1. This is a data breach class action against Defendant for its failure to adequately secure and safeguard Personally Identifiable Information ("PII").

2. On or about February 17, 2023, an unauthorized actor gained access to the Defendant's network and obtained unauthorized access to Defendant's files.[1] (the "Data Breach").

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/2b0ad8b2-8a7c-444e-836d-50025fd4dbb0.shtml (last viewed Nov. 7, 2023).

3. Upon information and belief, approximately 12,143 individuals' PII was affected by the Data Breach. The PII lost in the Data Breach included names, addresses, Social Security numbers, health insurance applications/claims information, and credit/debit card numbers.[2]

4. After learning of the incident, Defendant conducted an investigation and engaged outside cybersecurity professionals and data privacy counsel. Defendant, so far, has yet to inform affected individuals when it completed its investigation or when it completely learned of the extent of the Data Breach.

5. Upon information and belief, Defendant discovered the Data Breach on or about February 17, 2023.[3]

6. On or about September 15, 2023, Defendant began notifying affected individuals that their PII was impacted in the Data Breach.[4]

7. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to Plaintiff and the Class, to keep their PII confidential, safe, secure, and protected from unauthorized disclosure or access.

8. Plaintiff and the Class have taken reasonable steps to maintain the confidentiality and security of their PII.

[2] *Id.*
[3] *Id.*
[4] *Id.*

9. Plaintiff and the Class reasonably expected Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

10. Defendant, however, breached its numerous duties and obligations by failing to implement and maintain reasonable safeguards; failing to comply with industry-standard data security practices and federal and state laws and regulations governing data security; failing to properly train its employees on data security measures and protocols; failing to timely recognize and detect unauthorized third parties accessing its system and that substantial amounts of data had been compromised; and failing to timely notify the impacted Class.

11. In this day and age of regular and consistent data security attacks and data breaches and given the sensitivity of the data entrusted to Defendant, this Data Breach is particularly egregious and foreseeable.

12. By implementing and maintaining reasonable safeguards and complying with standard data security practices, Defendant could have prevented this Data Breach.

13. Plaintiff and the Class are now faced with a present and imminent lifetime risk of identity theft. These risks are made all the more substantial, and significant because of the inclusion of Social Security numbers and other static PII.

14. PII has great value to cyber criminals, especially Social Security numbers. As a direct cause of Defendant's Data Breach, Plaintiff's and the Class's PII is in the hands of cyber-criminals and may be available for sale on the dark web for other criminals to access and abuse at the expense of Plaintiff and the Class. Plaintiff and the Class face a

current and lifetime risk of imminent identity theft or fraud as a direct result of the Data Breach.

15. Defendant acknowledges the imminent threat the Data Breach has caused to Plaintiff and the Class and has provided reassurance that it is in the process of "reviewing and enhancing [their] existing policies and procedures related to data privacy to reduce the likelihood of a similar future event."[5]

16. The modern cyber-criminal can use the PII and information stolen in cyber-attacks to assume a victim's identity when carrying out various crimes such as:

a. Using a victim's credit history;

b. Making financial transactions on their behalf and without their knowledge, including opening credit accounts in their name or taking out loans;

c. Impersonating them in written communications, including mail e-mail and/or text messaging;

d. Stealing and using benefits that belong to the victim;

e. Committing illegal acts while impersonating them which, in turn, incriminate the victim.

17. Plaintiff's and the Class's PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect Plaintiff's and the Class's PII. Defendant not only failed to prevent the Data Breach, but after discovering the Data Breach in February 2023, Defendant waited until September 15, 2023, an

[5] *See* **Exhibit 1**.

unreasonable amount of time, to begin notifying state Attorney Generals and affected individuals, such as Plaintiff and members of the Class.

18. As a result of Defendant's delayed response to the data breach, Plaintiff and Class had no idea their PII had been compromised, and that they were, and continue to be, at significant and imminent risk of identity theft and various other forms of personal, social and financial harm. The risk will remain for their respective lifetimes because of Defendant's negligence.

19. Plaintiff brings this action on behalf of all persons whose PII was compromised because Defendant failed to:

(i) adequately protect consumers' PII entrusted to it,

(ii) warn its current and former customers, potential customers, and current and former employees of their inadequate information security practices, and

(iii) effectively monitor their websites and platforms for security vulnerabilities and incidents.

20. Defendant's conduct violates federal and state statutes and guidelines as well as its duties under common law.

21. As a result of the Data Breach, Plaintiff and Class suffered ascertainable losses, including but not limited to, a loss of privacy. These injuries include:

(i) the invasion of privacy;

(ii) the compromise, disclosure, theft, and imminent unauthorized use of Plaintiff's and the Class's PII;

(iii) emotional distress, fear, anxiety, nuisance and annoyance related to the theft and compromise of their PII;

(iv) lost or diminished inherent value of PII; out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time;

(v) the continued and increased risk to their PII, which, (a) remains available on the dark web for individuals to access and abuse; and (b) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and Class.

22. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of himself and all similarly situated persons whose PII was compromised and stolen as a result of the Data Breach and remains at risk due to inadequate data security.

23. Accordingly, Plaintiff, on behalf of himself and the Class, asserts claims for negligence, negligence *per se*, breach of implied contract, and unjust enrichment. Plaintiff seeks injunctive relief, declaratory relief, monetary damages, and all other relief as authorized in equity or by law.

PARTIES

24. Plaintiff Mary Cogan was and currently is a citizen of New York and at all relevant times and currently resides in Saratoga Springs, NY.

25. Defendant is a college located at 815 North Broadway, Saratoga Springs, NY 12866.[6]

26. Defendant is a four-year private, nonsectarian, coeducational school that has 2,700 undergraduate students and provides 44 majors, 19 athletic varsity teams, and more than 100 student organizations.[7]

27. Defendant collects and requires its students, applicants, and/or employees to provide PII in the course of operating as a higher educational institution.

28. By obtaining, collecting, using, and deriving benefit from Plaintiff's and Class's PII, Defendant assumed legal and equitable duties to those persons, and knew or should have known that it was responsible for protecting Plaintiff's and Class's PII from unauthorized disclosure and/or criminal hacking activity.

JURISDICTION AND VENUE

29. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d), *et seq*. The amount in controversy exceeds $5 million, exclusive of interest and costs. There are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant, including Plaintiff. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

[6] *Id*.
[7] https://www.skidmore.edu/about/

30. This Court has personal jurisdiction over Defendant because Defendant's principal places of business is located within this District and the Defendant conducts substantial business in this district.

31. Venue is proper in this Court under 28 U.S.C. § 1391, because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District, and Defendant resides within this judicial district.

FACTUAL ALLEGATIONS

Background

32. In the ordinary course of its business practices, Defendant stores, maintains, and uses Plaintiff's and Class Members' PII including but not limited to:

a. Full names;

b. Social Security numbers;

c. Address; and

d. Credit/debit card information.

33. Defendant understands the importance of securely maintaining PII.

34. Defendant's privacy policy, which was updated on October 4, 2023, explains that "Skidmore will not share your [PII] with third parties…."[8] Defendant claims it "is firmly committed to data security."[9]

[8] https://www.skidmore.edu/privacy-statement/index.php#:~:text=Skidmore%20will%20not%20share%20your,under%20%22Sharing%20Your%20Information.%22&text=If%20you%20use%20any%20comment,to%20send%20you%20unsolicited%20messages.

[9] *Id*.

The Data Breach

35. Defendant became aware of the Data Breach on or about February 17, 2023.

36. Defendant then made steps to secure its systems and retain independent cybersecurity experts to investigate the matter further but did not begin notifying affected individuals until September 15, 2023.

37. In disclosures to the Maine Attorney General, Defendant stated that the Data Breach was discovered on February 17, 2023.[10] Defendant waited almost seven months after learning of the Data Breach before beginning to notify affected individuals.

38. Additionally, though Plaintiff and Class have an interest in ensuring that their information remains protected, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures taken to ensure a breach does not occur again have not been shared with regulators or the Class.

Defendant Was Aware of the Data Breach Risks

39. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class, to keep their PII confidential and to protect it from unauthorized access and disclosure.

40. Plaintiff and Class provided their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with their obligations to employ reasonable care to keep such information confidential and secure from unauthorized access.

[10] *See* **Exhibit 1**.

41. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and data breaches preceding the date of the Data Breach.

42. Indeed, data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so the targets are aware of and prepared for a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and foreseeable to the public and to anyone in Defendant's industry, including Defendant.

43. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take substantial time, money, and patience to resolve.[11] Identity thieves use the stolen PII for a variety of crimes, including but not limited to, credit card fraud, telephone or utilities fraud, and bank and finance fraud.[12]

---

[11] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://www.myoccu.org/sites/default/files/pdf/taking-charge-1.pdf (last visited Nov. 7, 2023).

[12] *Id*. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

44. The PII of Plaintiff and the Class were taken by cyber criminals for the very purpose of engaging in identity theft, fraud, or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

45. Defendant knew, or should have known, the importance of safeguarding the PII of Plaintiff and the Class, including Social Security numbers, driver's license numbers and/or state identification numbers, and of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class as a result of a breach.

46. Plaintiff and the Class now face years of constant monitoring and surveillance of their financial and personal records. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII as a direct result of the Data Breach.

47. The injuries to Plaintiff and Class were directly and proximately caused by Defendant's own failure to implement or maintain adequate data security measures and best practices for safeguarding the PII of Plaintiff and the Class.

Defendant Failed to Comply with FTC Guidelines

48. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable and adequate data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

49. In 2022, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[13]

50. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

51. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission

[13] Ritchie, J. N. & A., & Jayanti, S.F.-T. and A. (2022, April 26). *Protecting personal information: A guide for business.* Federal Trade Commission. https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed Nov. 7, 2023)

Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

52. Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

53. To prevent and detect cyber-attacks, including the cyber-attack on Defendant's network that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government and FTC, the following measures:

a. Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of malware and how it is delivered;

b. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing;

c. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users;

d. Configure firewalls to block access to known malicious IP addresses;

e. Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system;

f. Set anti-virus and anti-malware programs to conduct regular scans automatically;

g. Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary;

h. Configure access controls—including file, directory, and network share permissions— with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares;

i. Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications;

j. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common malware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder;

k. Consider disabling Remote Desktop protocol (RDP) if it is not being used;

l. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy;

m. Execute operating system environments or specific programs in a virtualized environment; and

n. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

54. Defendant was at all times fully aware of its obligation to protect the PII of customers, prospective customers and employees. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards

55. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices. Best cybersecurity practices that are standard in the financial services industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

56. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5,

PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness. These frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber-attack and causing the Data Breach.

57. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach.

PII Holds Value to Cyber Criminals

58. Businesses, such as Defendant, that store PII are likely to be targeted by cyber criminals. Credit card, routing, and bank account numbers are highly sought data targets for hackers, but information such as date of birth, driver's license and Social Security numbers are even more attractive to cyber criminals; they are not easily destroyed or replaceable and can be easily used to perpetrate acts of identity theft and other types of fraud.

59. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web to obtain PII of other unknown individuals. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII

can be sold at a price ranging from $40 to $200, and banking details have a price range of $50 to $200.[14]

60. Social Security numbers, for example, are among the worst kind of PII to have stolen or otherwise compromised because they may be put to a variety of fraudulent uses and are difficult for an individual to change or otherwise repair once it's compromised. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems. [15]

61. What is more, it is no easy task to change or cancel a stolen or compromised Social Security number as is the case for several of the Class members in this action. An individual cannot obtain a new Social Security number without significant time, monetary investment, paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted and the only forms of remediation happens *after* the first incident of misuse; an individual must

[14] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Nov. 7, 2023).

[15] *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Nov. 7, 2023).

show evidence of actual, ongoing fraudulent activity to be eligible to submit an application requesting a new Social Security number with the SSA.

62. Furthermore, as the SSA warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[16]

63. Here, the unauthorized access by cyber criminals left them with the tools to perform the most thorough identity theft—they have obtained all the essential PII that can be used to mimic the identity of the victim. The PII of Plaintiff and the Class stolen in the Data Breach constitutes a dream for hackers or cyber criminals and a nightmare for Plaintiff and the Class. Stolen personal data of Plaintiff and the Class represents essentially one-stop shopping for identity thieves indefinitely.

64. The FTC has released its updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems,

---

[16] *Id.*

using intrusion detection programs, monitoring data traffic, and having in place a response plan.

65. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office ("GAO") Report to Congressional Requesters:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[17]

66. Companies recognize that PII is a valuable asset and a valuable commodity, but also necessary throughout the typical course of business with consumers. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other PII on a number of dark web Internet websites. The stolen PII of Plaintiff and the Class has a high value on both legitimate and black markets.

67. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

[17] *See* https://www.gao.gov/assets/gao-07-737.pdf (June 2007) at 29.

68. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns or other tax related forms and documents using an alias of their victim. Class members whose Social Security numbers have been compromised in the Data Breach now face a real, present, imminent and substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

69. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because those victims can file disputes, cancel or close credit and debit cards and/or accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not nearly impossible, to change — Social Security number, driver's license number or government-issued identification number, name, and date of birth are durable.

70. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[18]

[18] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem- hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Nov. 7, 2023).

71. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police or other emergency medical services. An individual may not know that their driver's license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

Plaintiff's and Class Members' Damages

72. Defendant has failed to provide any compensation for the unauthorized release and disclosure of Plaintiff's and the Class's PII other than offering 24 months of Experian IdentityWorks complimentary monitoring services to individuals involved in the Data Breach.[19]

73. 24 months of monitoring services is wholly inadequately given the lifetime of heightened risk of identity theft that Plaintiff and the Class Members will face due to Defendant's failure to secure and keep confidential their PII.

74. Plaintiff and the Class have been damaged by the compromise of their PII in the Data Breach.

75. Plaintiff and the Class presently face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

[19] *See* **Exhibit 1**.

76. Plaintiff and the Class have been, and currently face substantial risk of being targeted now and in the future, to phishing, data intrusion, and other illegality based on their PII being compromised in the Data Breach as potential fraudsters could use the information garnered to target such schemes more effectively against Plaintiff and the Class.

77. Plaintiff and the Class may also incur out-of-pocket costs for implementing protective measures such as purchasing credit monitoring fees, credit report fees, credit freeze fees, and other similar costs directly or indirectly related to the Data Breach.

78. Plaintiff and the Class also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in data breach cases.

79. Plaintiff and the Class have spent and will continue to spend significant amounts of time to monitor their financial accounts, credit score, and records for misuse.

80. Plaintiff and the Class have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

81. Moreover, Plaintiff and the Class have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of proper and adequate security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing

personal and financial information is not accessible online and that access to such data is password protected.

82. Further, as a result of Defendant's conduct, Plaintiff and the Class are forced to live with the anxiety that their PII —which contains the most intimate details about a person's life—may be disclosed to the entire world, whether physically or virtually, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

83. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and the Class have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm because of the Data Breach.

Plaintiff Cogan's Experience

84. Plaintiff Cogan received Defendant's Notice of Data Breach letter from Defendant on September 23, 2023, over seven months after the Data Breach was detected in February of 2023.

85. Plaintiff Cogan is a former student and employee of Defendant Skidmore College.

86. The Notice advised that the PII that could have been accessed included Plaintiff Cogan's name, address, Social Security Number, date of birth, credit/debit card number, health insurance/app claims info, and his health insurance policy number/subscriber number.[20]

[20] *See* **Exhibit 1**.

87. The Notice further advised that Defendant was in the process of implementing "additional security protocols designed to protect our network, email, environment, and systems."[21]

88. Prior to this Data Breach, Plaintiff Cogan had taken steps to protect against keeping his PII safe and monitored his PII closely. He has not knowingly transmitted his PII over unsecured or unencrypted internet connections.

89. Plaintiff has suffered actual damages and is at imminent, impending, and substantial risk for identity theft and future economic harm due to the highly sensitive nature of the information that was targeted and stolen in the Data Breach. Since learning about the breach, in an effort to mitigate the risk, Plaintiff has spent time and effort reviewing financial statements and identity theft protection reports to detect and prevent identity theft. Plaintiff has suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the theft and compromise of his PII. Plaintiff will continue to spend additional time and incur future economic costs associated with the detection and prevention of identity theft.

90. Plaintiff Cogan entrusted his PII and other confidential information to Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to his PII. Plaintiff Cogan would not have allowed Defendant

[21] *Id*.

to collect and maintain his PII had he known that Defendant would not take reasonable steps to safeguard his PII.

91. Plaintiff Cogan has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone calls, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This is time that has been lost forever and cannot be recaptured.

92. Plaintiff Cogan stores all documents containing his PII in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for the online accounts that he has.

93. Plaintiff Cogan has suffered actual injury in the form of damages to, and diminution in, the value of his PII – a form of intangible property that Plaintiff Cogan entrusted to Defendant. This PII was compromised in, and has been diminished as a result of, the Data Breach.

94. Plaintiff Cogan has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces.

95. Plaintiff Cogan has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII resulting from the compromise of his PII, especially his Social Security number, in combination with his

name, address, phone number, and email address, which PII is now in the hands of cyber criminals and other unauthorized third parties.

96. Knowing that thieves stole his PII, including his Social Security number and other PII that he was required to be provided to Defendant, and knowing that his PII will likely be sold on the dark web, has caused Plaintiff Cogan great anxiety.

97. Additionally, Plaintiff Cogan does not recall having been involved in any other data breaches in which his highly confidential PII, such as Social Security Number was compromised.

98. Plaintiff Cogan has a continuing interest in ensuring that his PII which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches.

99. As a result of the Data Breach, Plaintiff Cogan is presently and will continue to be at a present and heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

CLASS ALLEGATIONS

100. Plaintiff brings this nationwide class action according to Federal Rules of Civil Procedure, Rules 23(b)(2), 23(b)(3), and 23(c)(4).

101. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All persons residing in the United States whose PII was compromised during the Data Breach that is the subject of the Notice of Data Breach published by Defendant on or about September 15, 2023 (the "Class").

102. Excluded from the Class are: (i) Defendant and its employees, officers, directors, affiliates, parents, subsidiaries, and any entity in which Defendant has a whole

or partial ownership of financial interest; (ii) all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; (iii) any counsel and their respective staff appearing in this matter; and (iv) all judges assigned to hear any aspect of this litigation, their immediate family members, and their respective court staff.

103. Plaintiff reserves the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

104. **Numerosity**. The Class is so numerous that joinder of all members is impracticable. The Class includes thousands of individuals whose personal data was compromised by the Data Breach. The exact number of Class members is in the possession and control of Defendant and will be ascertainable through discovery, but Defendant has disclosed that approximately 12,143 individuals PII was involved in the Data Breach.

105. **Commonality.** There are numerous questions of law and fact common to Plaintiff and the Class that predominate over any questions that may affect only individual Class members, including, without limitation:

a. Whether Defendant unlawfully maintained, lost or disclosed Plaintiff's and Class's Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class to safeguard their Private Information;

f. Whether Defendant breached duties to Class to safeguard their Private Information;

g. Whether cyber criminals obtained Class's Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Defendant owed a duty to provide Plaintiff and Class timely notice of this Data Breach, and whether Defendant breached that duty;

j. Whether Plaintiff and Class suffered legally cognizable damages as a result of Defendant's misconduct;

k. Whether Defendant's conduct was negligent;

l. Whether Defendant's conduct violated federal law;

m. Whether Defendant's conduct violated state law; and

n. Whether Plaintiff and Class are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

106. **Typicality**. Plaintiff's claims are atypical of the claims of the Class in that Plaintiff, like all proposed Class members, had his PII compromised, breached, or otherwise stolen in the Data Breach. Plaintiff and the Class were injured through the

uniform misconduct of Defendant, described throughout this Complaint, and assert the same claims for relief.

107. **Adequacy**. Plaintiff and counsel will fairly and adequately protect the interests of Plaintiff and the proposed Class. Plaintiff retained counsel who are experienced in Class action and complex litigation, particularly those involving Data Breach as is at issue in this class action complaint. Plaintiff has no interests that are antagonistic to, or in conflict with, the interests of other Class members.

108. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiff and the Class have been harmed by Defendant's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Defendant's conduct and/or inaction. Plaintiff knows of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

109. Class certification is appropriate under Fed. R. Civ. P. 23(b)(1)(A), in that the prosecution of separate actions by the individual Class members would create a risk of inconsistent or varying adjudications with respect to individual members of the Class, which would establish incompatible standards of conduct for Defendant. In contrast, the

conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each member of the Class. Specifically, injunctive relief could be entered in multiple cases, but the ordered relief may vary, causing Defendant to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by Class members would create the risk of adjudications with respect to individual Class members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

110. Class certification, therefore, is appropriate under Rule 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

111. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed its legal duty or obligation to Plaintiff and the Class to exercise due care in collecting, storing, using, safeguarding, or otherwise maintaining their PII;

b. Whether Defendant breached its legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, safeguarding, or otherwise maintaining their PII;

c. Whether Defendant failed to comply with its own policies or procedures and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether Plaintiff and the Class are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Rule 23 Class)

112. Plaintiff and the Class re-allege and incorporate all foregoing paragraphs of this Complaint as if fully set forth herein.

113. Plaintiff and the Class entrusted Defendant with their PII.

114. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and not disclose their PII to unauthorized third parties.

115. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in obtaining, using, maintaining and protecting their PII from unauthorized third parties.

116. The legal duties owed by Defendant to Plaintiff and the Class include, but are not limited to the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiff and the Class in Defendants possession;

b. To protect PII of Plaintiff and the Class in Defendants possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. To implement processes and software to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and Class of the Data Breach.

117. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interested and enforced by the Federal Trade Commission, the unfair practices by companies such as Defendant of failing to use reasonable measures to protect PII.

118. Various FTC publications and data security breach orders further form the basis of Defendant's duty. Plaintiff and Class are consumers under the FTC Act. Defendant

violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and by not complying with industry standards.

119. Defendant breached its duties to Plaintiff and the Class. Defendant knew or should have known the risks of collecting and storing PII and the importance of maintaining secure systems, especially in light of the fact that data breaches have recently been prevalent.

120. Defendant knew or should have known that its security practices did not adequately safeguard the PII of Plaintiff and the Class.

121. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security measures and its failure to protect the PII of Plaintiff and the Class from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiff and the Class during the period it was within Defendant's possession and control.

122. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of obtaining services from Defendant.

123. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff and the class.

124. Defendant's own conduct created a foreseeable risk of harm to a individual, including Plaintiff and the Class. Defendant's misconduct included, but was not limited

to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included their decisions not to comply with industry standards for safekeeping of the PII of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

125. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

126. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Class.

127. Defendant breached the duties it owes to Plaintiff and Class in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect employees' and customers' PII and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards during the period of the Data Breach;

c. Failing to act despite knowing or having reason to know that its systems were vulnerable to attack; and

d. Failing to timely and accurately disclose to customers and employees that their PII had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

128. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was stolen and accessed as the proximate result of Defendant's failure to exercise reasonable care in

safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

129. Due to Defendant's misconduct, Plaintiff and the Class are entitled to credit monitoring at a minimum. The PII taken in the Data Breach can be used for identity theft and other types of financial fraud against Plaintiff and the Class.

130. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately $219 to $358 per year. To date, Defendant has only offered 24 months of "complimentary access to Experian IdentityWorksSM" [sic].

131. As a result of Defendant's negligence, Plaintiff and Class suffered injuries that include:

i. the lost or diminished value of PII;

ii. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII;

iii. lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account;

iv. the continued risk to their PII, which may remain for sale on the dark web and is in Defendant's possession and subject to further

unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII in their continued possession;

v. future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class, including ongoing credit monitoring.

132. These injuries were reasonably foreseeable given the history and uptick of data security breaches of this nature within the financial sector. The injury and harm that Plaintiff and the Class suffered was the direct and proximate result of Defendant's negligent conduct.

COUNT II
Negligence *Per Se*
(On Behalf of the Rule 23 Class)

133. Plaintiff and the Class re-allege and incorporate all foregoing paragraphs of this Complaint as if fully set forth herein.

134. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

135. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and comply with applicable industry standards. Defendant's

conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable harm.

136. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

137. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

138. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

139. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to

protect the PII of its current and former employees and customers in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

140. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

141. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Rule 23 Class)

142. Plaintiff and the Class re-allege and incorporate all foregoing paragraphs of this Complaint as if fully set forth herein.

143. Plaintiff's and Class Members' PII was provided to Defendant as a condition of receiving an education or being employed by Defendant.

144. When Plaintiff and Class Members provided their PII to Defendant as part of their receipt of education or employment, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties to protect their PII and to timely notify them in the event of a Data Breach.

145. Based on Defendant's legal obligations and acceptance of Plaintiff's and Class Members' PII, Defendant had an implied duty to safeguard their PII through the use of reasonable industry standards.

146. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class Members' PII and failing to provide them with timely and accurate notice of the Data Breach. Indeed, it took Defendant almost seven months to begin warning Plaintiff and Class Members of their imminent risk of identity theft.

147. As a direct and proximate result of Defendant's breach of implied contract, Plaintiff and the Class Members have suffered damages, including foreseeable consequential damages that Defendant knew about when it requested Plaintiff's and the Class Members' PII.

148. Plaintiff and the Class have suffered injury, and are entitled to actual and punitive damages, statutory damages, and reasonable attorneys' fees and costs, in an amount to be proven at trial.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Rule 23 Class)

149. Plaintiff and the Class re-allege and incorporate all foregoing paragraphs of this Complaint as if fully set forth herein. This Count is pled in the alternative to the Breach of Implied Contract Count above.

150. Plaintiff and the Class conferred a monetary benefit to Defendant by providing Defendant with their valuable PII, which Defendant knowingly used or retained in the course of its business.

151. Defendant benefited from receiving Plaintiff's and the Class members' PII by its ability to retain and use that information for its own financial business benefit. Defendant understood this benefit and accepted the benefit knowingly.

152. Defendant also understood and appreciated that the PII of Plaintiff and the Class was private and confidential to them, and that its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

153. Plaintiff and the Class conferred a monetary benefit upon Defendant in the form of monies paid to Defendant for services.

154. The monies paid to Defendant for services involving Plaintiff and the Class PII were to be used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

155. Defendant also understood that Plaintiff's and the Class's PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

156. But for Defendant's willingness and commitment to maintain privacy and confidentiality, that PII would not have been transferred to and entrusted with Defendant. Indeed, if Defendant had informed its customers that Defendant's data and cyber security measures were inadequate, Defendant would not have been permitted to continue to operate in that fashion by regulators, its shareholders, and its consumers.

157. As a result of Defendant's wrongful conduct, Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and the Class. Defendant

continues to benefit and profit from their retention and use of the PII while its value to Plaintiff and the Class has been diminished.

158. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged in this complaint, including compiling, using, and retaining Plaintiff and the Class's PII, while at the same time failing to maintain that information securely from intrusion and theft by cyber criminals, hackers and identity thieves.

159. Plaintiff and the Class have no adequate remedy at law.

160. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and the Class because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and the Class paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

161. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm. Defendant should be completed to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and the Class, proceeds that they unjustly received from them.

COUNT V
Declaratory Judgment and Injunctive Relief
(On Behalf of Plaintiff and the Rule 23 Class)

162. Plaintiff and the Class re-allege and incorporate all foregoing paragraphs of this Complaint as if fully set forth herein.

163. Plaintiff pursues this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

164. Defendant owes a duty of care to Plaintiff and the Class that require it to adequately secure Plaintiff's and the Class's PII.

165. Defendant failed to fulfill their duty of care to safeguard Plaintiff's and Class's the PII.

166. Plaintiff and the Class are at risk of harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

167. Plaintiff, therefore, seeks a declaration that (1) Defendant's existing security measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) to comply with their explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Conducting regular database scanning and security checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchasing credit monitoring services for Plaintiff and the Class for a period of ten years; and

h. Meaningfully educating Plaintiff and the Class about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, requests judgment against Defendant and that the Court grant the following:

1. For an order certifying the Class and appointing Plaintiff and her counsel to represent the Class;

2. For an order enjoining Defendant from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of the PII belonging to Plaintiff and the Class;

3. For injunctive relief requiring Defendant to:

   a. Engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

   b. Engage third-party security auditors and internal personnel to run automated security monitoring;

   c. Audit, test, and train its security personnel regarding any new or modified procedures;

   d. Segment their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

   e. Conduct regular database scanning and security checks;

   f. Routinely and continually conduct internal training and education to inform internal security personnel how to

identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchase credit monitoring services for Plaintiff and the Class for a period of ten years; and

h. Meaningfully educate Plaintiff and the Class about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

4. An order instructing Defendant to purchase or provide funds for credit monitoring services for Plaintiff and all Class members;

5. An award of compensatory, statutory, nominal and punitive damages, in an amount to be determined at trial;

6. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

7. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

8. Any and all such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands this matter be tried before a jury.

Respectfully submitted,

Dated: November 9, 2023

/s/ Randi Kassan
Randi Kassan

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza
Garden City, NY 11530
Telephone: (212) 594-5300
rkassan@milberg.com

William B. Federman*
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, OK 73120
Telephone: (405) 235-1560
-and-
212 W. Spring Valley Road
Richardson, TX 75081
wbf@federmanlaw.com

Attorneys for Plaintiff and Putative Class

**Pro Hac Vice forthcoming*

Exhibit 1

SKIDMORE
COLLEGE

Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

MARY COGAN
8 WILLOW LN
SARATOGA SPRINGS, NY 12866-3851

September 15, 2023
Rec'd 9/23

Dear Mary Cogan:

I am writing to inform you that we, Skidmore College ("Skidmore" or "we") recently experienced a data incident ("incident") which potentially involved your personal information ("Information"). This letter provides you with information about this incident, what information was involved and what you can do, if you choose, in response. Additionally, although we are unaware of any misuse of your Information or fraud in relation to the incident, as a precaution we also provide steps you can take to protect your Information.

What Happened? , why (7) months later?

On February 17, 2023, Skidmore received an alert of suspicious activity in its systems and immediately began an investigation and took steps to contain and remediate the situation. This included changing passwords, implementing new threat detection and monitoring software, notifying law enforcement, and engaging outside cybersecurity professionals and data privacy counsel to assist.

I was not asked to change password

The investigation found that an unauthorized actor gained access to the Skidmore network before deploying ransomware that encrypted a small percentage of its faculty and staff filesharing system. The investigation discovered that some business and finance files were at risk of exfiltration by the unauthorized actor. Accordingly, Skidmore engaged a third-party data mining team to perform a thorough review of the relevant data set for the presence of personal information. We then conducted a manual review of the data mining results to confirm the identities of the individuals whose information was potentially involved and gather contact information, where available in order to send this notification. There is currently no evidence that any information has been misused for identity theft or fraud in connection with the incident.

What Information Was Involved?

We determined that the following types of Information may have been impacted: name, address, Social Security Number· date of birth; credit/debit card number without password or security code; health insur app/claims info; health insur policy#/subscriber#.

What We Are Doing.

Upon becoming aware of the incident, we immediately implemented measures to further improve the security of our systems and practices. We worked with leading data privacy and security professionals to aid in our investigation and response and have reported this incident to relevant government agencies and federal law enforcement. We also implemented additional security protocols designed to protect our network, email environment and systems.

What Can You Do?

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for twenty-four (24) months. While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary twenty-four (24) month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

freeze my credit

- You must **enroll by 12/7/2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit.
- Provide your **activation code** [redacted]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [redacted] by 12/7/2023. Be prepared to provide engagement number B103893 as proof of eligibility for the Identity Restoration services by Experian.

While credit monitoring services are available to you at no cost for twenty-four (24) months, it is always recommended that you remain vigilant, regularly monitor free credit reports and review account statements, and that you report any suspicious activity to financial institutions. Please also review the "Additional Resources" section included with this letter, which outlines other resources you can utilize to protect your Information.

For More Information.

We take this incident and the security of information in our care seriously. If you have any questions about the incident, please call [redacted], Monday through Friday, from 9:00 a.m. to 7:00 p.m. Eastern.

Sincerely,

9/

[redacted]

Dwane Sterling
Chief Technology Officer
Skidmore College

SKID-ADT-2Y

9/28/23

ADDITIONAL RESOURCES

How to freeze;

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

[redacted]

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You may obtain a security freeze on your credit report, free of charge, to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report, free of charge, or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

For New Mexico Residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Alabama Residents: You may contact the Attorney General's Office for the State of Alabama, Consumer Protection Division, 501 Washington Avenue, Montgomery, AL 36104, www.oag.state.md.us, 1-800-392-5658.

For District of Columbia Residents: You may contact the District of Columbia Office of the Attorney General, 400 6th Street NW, Washington, D.C. 20001, consumer.protection@dc.gov, (202) 442-9828.

For Illinois Residents: You may contact the Illinois Office of the Attorney General, 100 West Randolph Street, Chicago, IL 60601, https://illinoisattorneygeneral.gov/about/email_ag.jsp, 1-800-964-3013.

For Iowa Residents: You may contact the Iowa Office of the Attorney General, 1305 E. Walnut Street, Des Moines IA 50319, consumer@ag.iowa.gov, 1-888-777-4590.

For Kansas Residents: You may contact the Kansas Office of the Attorney General, Consumer Protection Division, 120 SW 10th Ave, 2nd Floor, Topeka, KS 66612-1597, https://ag.ks.gov/, 1-800-432-2310.

For Kentucky Residents: You may contact the Kentucky Office of the Attorney General, Consumer Protection Division, 1024 Capital Center Drive, Suite 200, Frankfort, Kentucky 40601, www.ag.ky.gov, 1-800-804-7556.

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For Minnesota Residents: You may contact the Minnesota Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For Missouri Residents: You may contact the Missouri Office of the Attorney General, Consumer Protection, 207 W. High St., P.O. Box 899, Jefferson City, MO 65102, www.ago.mo.gov, 1-800-392-8222.

For New Mexico Residents: You may contact the New Mexico Office of the Attorney General, Consumer Protection Division, 408 Galisteo Street, Villagra Building, Santa Fe, NM 87501, www.nmag.gov, 1-844-255-9210.

For New York Residents: You may contact the New York Office of the Attorney General, Office of the Attorney General, The Capitol, Albany, NY 12224-0341, https://ag.ny.gov, 1-800-771-7755.

For North Carolina Residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Main Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7266.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, Consumer Protection Division, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 1-401-274-4400.

For Texas Residents: You may contact the Texas Office of the Attorney General, Office of the Attorney General, PO Box 12548, Austin, TX 78711-2548, www.texasattorneygeneral.gov, 1-800-621-0508.

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa Residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts Residents: You have the right to obtain a police report if you are a victim of identity theft.

For North Carolina Residents: You are advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Oregon Residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island Residents: Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.